

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-143443

(43) 公開日 平成10年(1998) 5月29日

(51) Int. Cl.⁴
G 0 6 F 12/14
3/06
13/10

識別記号
3 2 0
3 0 4
3 4 0

F I
G 0 6 F 12/14
3/06
13/10

3 2 0 C
3 0 4 H
3 4 0 A

審査請求 未請求 請求項の数12 O L (全 12 頁)

(21) 出願番号 特願平8-305016

(22) 出願日 平成8年(1996)11月15日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 前田 真弓

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

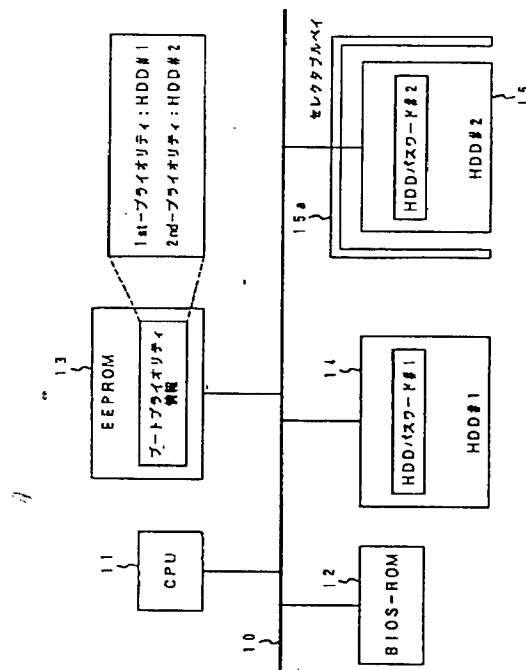
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 コンピュータシステムおよび同システムにおけるハードディスクパスワード制御方法

(57) 【要約】

【課題】 複数のハードディスクドライブが搭載されたシステムに最適なHDDパスワードチェック処理を実現する。

【解決手段】 システムのパワーオン時にCPU 11によって最初に実行されるPOSTは、1st-プライオリティのHDD 14がHDDパスワードチェックによりそれがアクセス可能状態となれば、2nd-プライオリティのHDD 15の状態とは無関係にブートストラップを実行する。したがって、ユーザは、必要最小限のパスワード、つまりブートデバイスとして使用されるHDD 14のパスワードさえ知っていればコンピュータを利用することができるようになる。また、2nd-プライオリティのHDD 15についても正当なパスワードが入力された場合にはそのデータの読み出しや更新を行うことができる。



【特許請求の範囲】

【請求項1】 パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、

前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、

前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、

前記第1のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記第1のハードディスクドライブ以外の他のハードディスクドライブそれぞれの状態とは無関係に、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とするコンピュータシステム。

【請求項2】 前記第1のハードディスクドライブのデータロック機能が解除されないとき、前記コンピュータシステムを強制的にパワーオフする手段をさらに具備することを特徴とする請求項1記載のコンピュータシステム。

【請求項3】 パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、

前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可

能にするパスワード制御処理を実行する手段と、

前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、

前記第1のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とするコンピュータシステム。

【請求項4】 前記複数のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、前記コンピュータシステムを強制的にパワーオフする手段をさらに具備することを特徴とする請求項2記載のコンピュータシステム。

【請求項5】 コンピュータ本体とコンピュータ本体に着脱自在に装着可能な拡張ユニットとを有し、ハードディスクドライブを増設するための機構が前記コンピュータ本体または前記拡張ユニットに設けられているコンピュータシステムであって、

パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、

前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、

前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、

前記第1のハードディスクドライブが動作可能で、且つ前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、そのデータロック機能が解除されないドライブが前記拡張ユニット上に存在するドライブであるか否かを判別する手段と、前記拡張ユニットに存在するドライブであることが検出されたとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とするコン

ピュータシステム。

【請求項6】 前記データロック機能が解除されないドライブが前記コンピュータ本体に存在しているとき、前記コンピュータシステムを強制的にパワーオフする手段をさらに具備することを特徴とする請求項5記載のコンピュータシステム。

【請求項7】 パスワードが設定可能に構成され、パスワードが設定されているときそのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおけるパスワード制御方法であって、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別し、

前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行し、

前記第1のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行した後、前記コンピュータシステムのブートストラップを実行することを特徴とするパスワード制御方法。

【請求項8】 前記第1のハードディスクドライブのデータロック機能が解除されないとき、前記コンピュータシステムを強制的にパワーオフすることを特徴とする請求項7記載のパスワード制御方法。

【請求項9】 パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおけるパスワード制御方法であって、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別し、

前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行し、

前記第1のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行した後、前記第1のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるか否かを検出し、

前記第1のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるとき、前記コンピュータシステムのブートストラップを実行することを特徴とするパスワード制御方法。

【請求項10】 前記第1のハードディスクドライブのデータロック機能が解除されないとき、および前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、前記コンピュータシステムを強制的にパワーオフすることを特徴とする請求項9記載のパスワード制御方法。

【請求項11】 コンピュータ本体とコンピュータ本体に着脱自在に装着可能な拡張ユニットとを有し、ハードディスクドライブを増設するための機構が前記コンピュータ本体または前記拡張ユニットに設けられているコンピュータシステムであって、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおけるパスワード制御方法であって、

前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別し、

前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行し、

前記第1のハードディスクドライブが動作可能状態であるとき、前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行し、

前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、そのデータロック機能が解除されないドライブが前記拡張ユニット上に存在するドライブであるか否かを判別し、

前記拡張ユニットに存在するドライブであることが検出されたとき、前記コンピュータシステムのブートストラ

ップを実行することを特徴とするパスワード制御方法。

【請求項12】 前記第1のハードディスクドライブのデータロック機能が解除されないとき、および前記他のハードディスクドライブの中のデータロック機能が解除されないドライブが前記コンピュータ本体に存在しているとき、前記コンピュータシステムを強制的にパワーオフすることを特徴とする請求項11記載のパスワード制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はコンピュータシステムおよびパスワード制御方法に関し、特にハードディスクドライブに設定されるHDDパスワードを用いてそのデータのセキュリティを保持するコンピュータシステムおよびHDDパスワードの制御方法に関する。

【0002】

【従来の技術】近年、ノートブックタイプおよびサブノートタイプの各種ポータブルコンピュータが開発されている。この種のポータブルコンピュータはその持ち運びが用意であるため、コンピュータ本体ごと盗難される危険がある。この場合、コンピュータ本体からその本体に内蔵されているハードディスクドライブを取り外し、そしてそのハードディスクドライブを他のコンピュータからアクセスすることなどによって、そのハードディスクドライブ内のデータを不正に読み出すことが可能となる。特に、コンピュータ本体に取り外し自在に装着できるバック型のハードディスクドライブについては、コンピュータ本体から簡単にハードディスクドライブを取り外すことができるため、不正なデータ読み出し操作やデータ書き換え操作を行うことはきわめて容易である。

【0003】そこで、最近では、ドライブ自体にパスワード（HDDパスワード）が設定可能に構成され、ユーザから正当なパスワードが入力されるまでデータアクセス操作を禁止するというデータロック機能を持つハードディスクドライブが開発され始めている。このハードディスクドライブのデータロック機能の仕組みは、USP5,375,243号公報に開示されている。現在では、このUSP5,375,243号公報と同等のデータロック機能はIDEインタフェースを持つハードディスクドライブの標準仕様としてその策定作業が進められている。

【0004】この種のハードディスクドライブを使用した典型的なHDDパスワードチェック処理では、まず、ソフトウェアの制御により、ハードディスクドライブにHDDパスワードが設定されているか否かが調べられ、設定されていれば、ユーザに対してパスワードの入力が促される。ユーザからパスワードが入力されると、その入力パスワードとハードディスク内のHDDパスワードとの照合がソフトウェアまたはハードディスクドライブ自体によって行われ、一致すると、ハードディスクドラ

イブのデータロック機能が自動的またはソフトウェア制御の下で解除され、そのデータアクセス操作が可能となる。

【0005】したがって、データロック機能を持つハードディスクドライブを使用した場合には、正当なパスワードを入力しない限り、その記憶データを読み出したリ、更新することが禁止されるため、そのデータ内容の機密性を保持することができる。

【0006】

【発明が解決しようとする課題】ところで、最近では、ポータブルコンピュータにおいてもデスクトップ型コンピュータと同等の性能および拡張性が要求されており、2台目のハードディスクドライブとCD-ROMドライブとを選択的に増設可能なセレクトابلベイを有するポータブルコンピュータや、ドッキングステーション等と称される専用の拡張ユニットを用いてその拡張ベイに収容されているハードディスクドライブを2台目のハードディスクドライブとして使用可能なポータブルコンピュータなどが開発されている。

【0007】このようにコンピュータ本体やドッキングステーションに増設されるハードディスクドライブについても、前述したデータロック機能を持つタイプのハードディスクドライブを使用することができる。

【0008】しかし、前述した従来のパスワードチェック機能は、ハードディスクドライブ毎にHDDパスワードを個々に照合するだけのものであるため、システムに搭載されているどのハードディスクドライブに対しても共通のパスワードチェックが行われる。このため、オペレーティングシステムを格納したハードディスクであるか否かや、コンピュータ本体とドッキングステーションのどちらに接続されたハードディスクドライブであるかなど、ハードディスクドライブそれぞれの用途の違いやその接続環境の違いなどを考慮したセキュリティ管理を行うことはできなかった。

【0009】この発明はこのような点に鑑みてなされたもので、データロック機能を有する複数のハードディスクドライブを使用可能な環境下においてそれらハードディスクドライブそれぞれの用途の違いやその接続環境の違いなどを考慮したパスワードチェック処理を実行できるようにし、システム全体の総合的なセキュリティレベルを向上することが可能なコンピュータシステムおよびHDDパスワード制御方法を提供することを目的とする。

【0010】

【課題を解決するための手段】請求項1に係る発明は、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、前記コンピ

ユータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、前記第1のハードディスクドライブがデータアクセス操作可能な状態であるとき、前記第1のハードディスクドライブ以外の他のハードディスクドライブそれぞれの状態とは無関係に、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とする。

【0011】このコンピュータシステムにおいては、コンピュータシステムがパワーオンされた時に最初に行われるPOST (Power-On Self Test) プログラムなどを用いて、以下のHDDパスワード制御処理が行われる。すなわち、コンピュータシステムがパワーオンされると、まず、POSTプログラムが、複数のハードディスクドライブの中でブート優先順位が最も高いハードディスクドライブ、つまりブートデバイスとして使用されるハードディスクドライブについて、パスワードの設定の有無が調べられる。パスワードが設定されていれば、パスワード入力用ウィンドウの表示などによって、パスワードの入力がユーザに促される。パスワードが入力されると、その入力パスワードとハードディスクドライブに設定されているパスワードとの一致の有無がPOST、あるいはハードディスクドライブ内部で調べられ、一致したときのみデータロック状態が解除される。これにより、ブートデバイスとして使用されるハードディスクドライブについては、パスワードが設定されていないか、あるいは正当なパスワードが入力された時にアクセス可能状態となる。ブートデバイス以外の他のハードディスクドライブそれぞれに対しても、同様にしてパスワード設定の有無の検出、および入力パスワードに基づいてデータロック状態を解除するためのパスワード制御処理が実行される。そして、この後、ブートデバイスとして使用されるハードディスクドライブがアクセス可能状態であるならば、他のハードディスクドライブそれぞれの状態によらず、ブートストラップが実行され、ブートデバイスとして使用されるハードディスクドライブからオペレーティングシステムが起動される。

【0012】このように、ブートデバイスとして使用さ

れるハードディスクドライブがアクセス可能状態であれば、他のハードディスクドライブそれぞれの状態とは無関係にブートストラップを実行することにより、ユーザは、必要最小限のパスワード、つまりブートデバイスとして使用されるハードディスクドライブのパスワードさえ知っていればコンピュータを利用することができるようになる。この場合、他のハードディスクドライブについても正当なパスワードが入力されたものについてはそのデータの読み出しや更新を行うことができ、また正当なパスワードが入力されなかったものについてはブート後においてもそのデータ内容の読み出しや更新は禁止されることになる。したがって、ハードディスクドライブそれぞれの用途の違いを考慮したパスワードチェック処理を実行できるようになり、システム全体の総合的なセキュリティレベルの向上とユーザの利便性とを両立することができる。

【0013】また、請求項2に係る発明においては、ブートデバイスとして使用されるハードディスクドライブに対応する正当なパスワードが入力されず、そのデータロック機能を解除できなかった場合には、そのままブートストラップ処理に移行してもそのハードディスクドライブからオペレーティングシステムを起動することはできないので、他のハードディスクドライブに対するパスワード制御処理およびブートストラップ処理を行うことなく、ブートデバイスに対する正当なパスワードが入力されなかった時点でコンピュータシステムを強制的にパワーオフすることを特徴とする。

【0014】ブートストラップ処理では、通常、複数のハードディスクドライブの中で最もブート優先順位の高いハードディスクドライブからオペレーティングシステムが起動されるが、多くのコンピュータでは、ブートストラップ処理時にフロッピーディスクが装着されていると、そのフロッピーディスクからオペレーティングシステムが起動されるように構成されている。したがって、請求項2のようにブートストラップ処理が実行される前にシステムを強制的にパワーオフすることは、ブートデバイスとして使用されるハードディスクドライブのパスワードを知らない人、つまり不正者によるフロッピーディスクなどを用いたブートストラップ処理の防止を図ることができる。

【0015】また、請求項3に係る発明は、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、前記第1のハードデ

ィスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、前記第1のハードディスクドライブと前記他のハードディスクドライブすべてがデータアクセス操作可能な状態であるとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とする。

【0016】このコンピュータシステムにおいては、セキュリティレベルをさらに向上させるために、ブートデバイスとして使用されるハードディスクドライブのみならず、それ以外の他のすべてのハードディスクドライブがアクセスが可能であるときのみブートストラップが実行される。したがって、すべてのハードディスクドライブについて正しいパスワードを知っているユーザに対してのみコンピュータの使用を許可することができる。

【0017】また、請求項5に係る発明は、コンピュータ本体とコンピュータ本体に着脱自在に装着可能な拡張ユニットとを有し、ハードディスクドライブを増設するための機構が前記コンピュータ本体または前記拡張ユニットに設けられているコンピュータシステムであって、パスワードが設定可能に構成され、パスワードが設定されているとき、そのパスワードがユーザから入力されるまでデータアクセス操作の実行を禁止するデータロック機能をそれぞれ有する複数のハードディスクドライブを使用可能なコンピュータシステムにおいて、前記コンピュータシステムのパワーオン時に、前記複数のハードディスクドライブの中で最も高いブート優先順位が割り当てられている第1のハードディスクドライブにパスワードが設定されているか否かを判別する手段と、前記第1のハードディスクドライブにパスワードが設定されているとき、ユーザにパスワードの入力を促し、ユーザからの入力パスワードと前記設定パスワードとが一致したときに前記第1のハードディスクドライブに前記データロック機能を解除させてデータアクセス操作を可能にするパスワード制御処理を実行する手段と、前記第1のハードディスクドライブ以外の他のハードディスクドライブの各々についてパスワード設定の有無を調べ、パスワードが設定されているハードディスクドライブに対して前記パスワード制御処理を実行する手段と、前記第1のハードディスクドライブが動作可能で、且つ前記他のハードディスクドライブの中にデータロック機能が解除されないドライブが存在するとき、そのデータロック機能が解除されないドライブが前記拡張ユニット上に存在する

ドライブであるか否かを判別する手段と、前記拡張ユニットに存在するドライブであることが検出されたとき、前記コンピュータシステムのブートストラップを実行する手段とを具備することを特徴とする。

【0018】このコンピュータシステムにおいては、ブートデバイス以外の他のハードディスクドライブが拡張ユニットに存在するものであるか、コンピュータ本体に存在するものであるかによってブート制御が切り替えられ、拡張ユニットに存在するものであればそのデータロック状態を解除できない場合であってもブートストラップ処理は実行される。これにより、例えばネットワーク接続された拡張ユニットがオフィス内に幾つか設置されており、その拡張ユニットにユーザ自身のコンピュータを装着してデータ通信などを行う場合は、拡張ユニット内に設けられた他人のハードディスクドライブの機密性を維持したまま、拡張ユニットの通信機能を利用するといった運用が可能となる。

【0019】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図1には、この発明の一実施形態に係るコンピュータシステムの構成が示されている。このコンピュータシステムはノートブックタイプのポータブルコンピュータであり、そのコンピュータ本体には、図示のように、システムバス10、CPU11、BIOS-ROM12、EEPROM13、およびハードディスクドライブ(HDD=1)14が内蔵されている。さらに、そのコンピュータ本体には、ハードディスクドライブまたはCD-ROMドライブを選択的に増設するためのセレクトابلベイ15aが設けられており、この実施形態では、セレクトابلベイ15aには2台目のハードディスクドライブ(HDD=2)15が収容されている。

【0020】ハードディスクドライブ(HDD=1)14はIDE規格のATAドライブであり、データロック機能を有している。このデータロック機能は、パスワード設定プログラム等を用いてユーザがハードディスクドライブ(HDD=1)14内にHDDパスワード=1を予め登録しておくことによって有効となり、HDDパスワード=1と一致するパスワードが入力された時に解除される。データロック機能が有効な状態においては通常のデータリード/ライトに関するコマンドは一切受け付けられず、これによりデータアクセス操作の実行が禁止される。

【0021】ハードディスクドライブ(HDD=2)15もハードディスクドライブ(HDD=1)14と同じデータロック機能を有しており、HDDパスワード=2を設定しておくことにより、そのパスワードが入力されるまではデータアクセス操作を禁止することができる。

【0022】CPU11は、このシステム全体の動作を制御するものであり、オペレーティングシステムおよび

各種アプリケーションプログラムを初め、BIOS-ROM12に格納されたシステムBIOSを実行する。このシステムBIOSには、コンピュータシステムのパワーオン時に最初に実行されるPOSTプログラムが含まれており、HDDのデータロック機能を利用するためのパスワード制御処理はこのPOSTプログラムによって実行される。

【0023】パスワード制御処理はハードディスクドライブ14、15に記憶されているデータやプログラムの不正使用および書き換えを防止するためのものであるが、この実施形態では、さらに、セキュリティレベルの向上のために、ブートデバイスとして使用されるハードディスクドライブのデータロックが解除できない場合はブートストラップを実行せずにシステムを強制的にパワーオフする仕組みが設けられている。パスワード制御処理の詳細な手順は図3乃至図5のフローチャートを参照して後述する。

【0024】ハードディスクドライブ14、15のどちらをブートデバイスとして使用するかは、EEPROM13に設定されているブート優先順位情報によって決定される。このブート優先順位情報はオペレーティングシステムを起動するハードディスクの順番を規定するものであり、環境設定プログラムなどを用いることによりユーザが自由に書き換えることができる。図1のブート優先順位情報においてはハードディスクドライブ14、15の順でブート優先順位が割り当てられており、この場合には、ハードディスクドライブ14が1stプライオリティのHDD（ブートデバイス）、ハードディスクドライブ14が2ndプライオリティのHDDとなる。

【0025】この実施形態のパスワード制御処理は、以上のようなシステム構成、つまり、以下の条件下で動作することを前提としている。

- (1) データロック機能を有するハードディスクドライブをサポートするシステムである。
- (2) データロック機能を有するハードディスクドライブが2台またはそれ以上接続されている。
- (3) 2台またはそれ以上のハードディスクドライブに対してブート優先順位を割り当てることができ、1stプライオリティのHDDと2ndプライオリティ以降のHDDが明確化されている。

【0026】以上の条件は、2台目以降のハードディスクドライブをコンピュータ本体ではなく、図2に示されているように、ドッキングステーション30に収容して使用する場合でも満足される。

【0027】図2のシステムにおいては、コンピュータ本体を取り外し自在に装着できるドッキングステーション30のセレクトابلベイ15aにハードディスクドライブ15が収容されている。コンピュータ本体をコネクタ20を介してドッキングステーション30に接続した

場合には、コンピュータ本体は2台のハードディスクドライブを持つシステム構成に機能拡張されることになる。

【0028】また、図1のポータブルコンピュータ本体を図2のドッキングステーション30に接続し、3台のハードディスクドライブを持つシステム構成として使用することも可能である。

【0029】次に、図3のフローチャートを参照して、POSTプログラムによって実行されるパスワード制御処理の第1の例を説明する。コンピュータがパワーオンされると、CPU11によって最初にPOSTプログラムが実行され、そのPOSTプログラムの制御の下でメモリおよびハードウェアテストが行われ、その処理が正常終了するとブートストラップが開始される。パスワード制御処理はシステムに接続されているハードディスクドライブのテストおよび初期化時に以下の手順で実行される。

【0030】POSTプログラムは、まず、EEPROM13のブート優先順位情報からブートデバイスとなるハードディスクドライブ（1stプライオリティのHDD14）を認識し、その1stプライオリティのHDD14にHDDパスワードが設定されているか否かを調べる（ステップS101）。これは、1stプライオリティのHDD14がデータロック状態か否かを問い合わせるステータスリードコマンドをHDD14に発行することによって行うことができる。1stプライオリティのHDD14にHDDパスワードが設定されている場合は、POSTプログラムは、パスワード入力ウィンドウを画面表示し、パスワードの入力をユーザに促す（ステップS102）。

【0031】パスワードが入力されると、POSTプログラムは、1stプライオリティのHDD14から読み取ったHDDパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップS103）。正しいならば、POSTプログラムは、1stプライオリティのHDD14にデータロック解除コマンドを送ることによりHDD14にデータロック状態を解除させ、HDD14をデータアクセス可能状態にする（ステップS105）。入力パスワードが正しくない場合には、1stプライオリティのHDD14のデータロック状態は解除できないので、HDD14からオペレーティングシステムを起動することはできない。このため、POSTプログラムは、セキュリティレベルの向上も考慮して、コンピュータシステムを強制的にパワーオフする（ステップS104）。このようにブートストラップ処理を実行する前にシステムをパワーオフすることにより、不正者によるフロッピーディスクなどを用いたオペレーティングシステムの起動を防止することができる。

【0032】HDD14がパスワード照合機能を持つ場

合には、ステップS103ではPOSTプログラムはHDD14にパスワードを入力するだけで良く、またパスワードが一致した場合にはHDD14内でデータロック機能が自動的に解除されるので、ステップS105の処理は不要となる。パスワードの一致の有無は、POSTプログラムがHDD14にステータスリードコマンドを発行してデータロック状態か否かを調べることなどによって認識することができる。

【0033】HDD14のデータロック状態が解除されたとき、またはHDD14にHDDパスワードが設定されていなかったときは、2ndプライオリティのHDD15に対して同様の処理が実行される。

【0034】すなわち、POSTプログラムは、2ndプライオリティのHDD15にHDDパスワードが設定されているか否かを調べる（ステップS106）。2ndプライオリティのHDD15にHDDパスワードが設定されている場合は、POSTプログラムは、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップS107）。パスワードが入力されると、POSTプログラムは、2ndプライオリティのHDD15から読み取ったHDDパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップS108）。正しいならば、POSTプログラムは、2ndプライオリティのHDD15にデータロック解除コマンドを送ることによりHDD15にデータロック状態を解除させ、HDD15をデータアクセス可能状態にする（ステップS109）。ステップS108およびステップS109は、前述したHDD14の場合と同様にし、HDD15自体のパスワード照合機能を利用して行うこともできる。

【0035】この後、POSTプログラムは、HDD15のデータロック状態が解除されたか否か、およびHDD15にパスワードが設定されていたか否かに関わらず、ブートストラップ処理を実行する（ステップS110）。このブートストラップ処理はPOSTプログラムによって起動されるシステムBIOS内のブートアッププログラムによって実行され、1stプライオリティのHDD14からオペレーティングシステムが主記憶上にロードされる。

【0036】以上のように、図3のパスワード制御処理の手順においては、1stプライオリティのHDD14がアクセス可能状態であれば、2ndプライオリティのHDD15の状態とは無関係にブートストラップを実行される。したがって、ユーザは、必要最小限のパスワード、つまりブートデバイスとして使用されるHDD14のパスワードさえ知っていればコンピュータを利用することができるようになる。また、2ndプライオリティのHDD15についても正当なパスワードが入力された場合にはそのデータの読み出しや更新を行うこと

ができ、また正当なパスワードが入力されなかった場合にはブート後においてもそのデータ内容の読み出しや更新は禁止されることになる。したがって、ハードディスクドライブ14、15それぞれのブート優先順位を考慮したパスワードチェック処理を実行できるようになり、システム全体の総合的なセキュリティーレベルの向上とユーザの利便性とを両立することができる。

【0037】次に、図4のフローチャートを参照して、POSTプログラムによって実行されるパスワード制御処理の第2の例を説明する。このパスワード制御処理は、図3の処理よりもさらにセキュリティーレベルを高めることを目的としており、1stプライオリティのHDD14および2ndプライオリティのHDD15の双方がアクセス可能状態になったときに初めてブートストラップを実行する構成である。

【0038】すなわち、コンピュータがパワーオンされると、POSTプログラムは、1stプライオリティのHDD14にHDDパスワードが設定されているか否かを調べ（ステップS201）、HDD14にHDDパスワードが設定されている場合は、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップS202）。パスワードが入力されると、POSTプログラムは、1stプライオリティのHDD14から読み取ったHDDパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップS203）。正しいならば、POSTプログラムは、1stプライオリティのHDD14にデータロック解除コマンドを送ることによりHDD14にデータロック状態を解除させ、HDD14をデータアクセス可能状態にする（ステップS205）。入力パスワードが正しくない場合には、1stプライオリティのHDD14のデータロック状態は解除できないので、HDD14からオペレーティングシステムを起動することはできない。このため、POSTプログラムは、セキュリティーレベルの向上も考慮して、コンピュータシステムを強制的にパワーオフする（ステップS204）。

【0039】HDD14のデータロック状態が解除されたとき、またはHDD14にHDDパスワードが設定されていなかったときは、2ndプライオリティのHDD15に対して以下の処理が行われる。

【0040】すなわち、POSTプログラムは、2ndプライオリティのHDD15にHDDパスワードが設定されているか否かを調べる（ステップS206）。2ndプライオリティのHDD15にHDDパスワードが設定されている場合は、POSTプログラムは、パスワード入力ウインドウを画面表示し、パスワードの入力をユーザに促す（ステップS207）。パスワードが入力されると、POSTプログラムは、2ndプライオリティのHDD15から読み取ったHDDパスワードと

ユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップS208）。正しいならば、POSTプログラムは、2ndプライオリティのHDD15にデータロック解除コマンドを送ることによりHDD15にデータロック状態を解除させ、HDD15をデータアクセス可能状態にする（ステップS209）。

【0041】この後、POSTプログラムは、HDD15のデータロック状態が解除されたか、あるいはHDD15にパスワードが設定されていたか場合、つまりHDD14およびHDD15の双方がアクセス可能状態であることを条件に、ブートストラップ処理を実行する（ステップS210）。1stプライオリティのHDD14がアクセス可能状態であっても、2ndプライオリティのHDD15のデータロック状態が解除できない場合は、システムが強制的にパワーオフされる（ステップS211）。

【0042】次に、図5のフローチャートを参照して、POSTプログラムによって実行されるパスワード制御処理の第3の例を説明する。このパスワード制御処理では、1stプライオリティのHDDがアクセス可能状態で、且つ2ndプライオリティ以降のHDDの中にデータロック状態を解除できないHDDがある場合に、そのHDDがドッキングステーションとコンピュータ本体のどちらに設けられているものであるかが調べられ、ドッキングステーションに設けられているものであったときにブートストラップが許可される。

【0043】すなわち、コンピュータがパワーオンされると、POSTプログラムは、1stプライオリティのHDD14にHDDパスワードが設定されているか否かを調べ（ステップS301）、HDD14にHDDパスワードが設定されている場合は、パスワード入力ウィンドウを画面表示し、パスワードの入力をユーザに促す（ステップS302）。パスワードが入力されると、POSTプログラムは、1stプライオリティのHDD14から読み取ったHDDパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップS303）。正しいならば、POSTプログラムは、1stプライオリティのHDD14にデータロック解除コマンドを送ることによりHDD14にデータロック状態を解除させ、HDD14をデータアクセス可能状態にする（ステップS305）。入力パスワードが正しくない場合には、1stプライオリティのHDD14のデータロック状態は解除できないので、HDD14からオペレーティングシステムを起動することはできない。このため、POSTプログラムは、セキュリティレベルの向上も考慮して、コンピュータシステムを強制的にパワーオフする（ステップS304）。

【0044】HDD14のデータロック状態が解除され

たとき、またはHDD14にHDDパスワードが設定されていなかったときは、2ndプライオリティのHDD15に対して以下の処理が行われる。

【0045】すなわち、POSTプログラムは、2ndプライオリティのHDD15にHDDパスワードが設定されているか否かを調べる（ステップS306）。2ndプライオリティのHDD15にHDDパスワードが設定されている場合は、POSTプログラムは、パスワード入力ウィンドウを画面表示し、パスワードの入力をユーザに促す（ステップS307）。パスワードが入力されると、POSTプログラムは、2ndプライオリティのHDD15から読み取ったHDDパスワードとユーザからの入力パスワードとを照合し、入力パスワードが正しいか否かを調べる（ステップS308）。正しいならば、POSTプログラムは、2ndプライオリティのHDD15にデータロック解除コマンドを送ることによりHDD15にデータロック状態を解除させ、HDD15をデータアクセス可能状態にする（ステップS309）。そして、ブートストラップ処理が実行される（ステップS312）。

【0046】一方、2ndプライオリティのHDD15のデータロック状態が解除できない場合には、POSTプログラムは、そのHDD15がコンピュータ本体とドッキングステーションのどちらに設けられているかを検出し（ステップS310）、コンピュータ本体に設けられたものであれば、その時点でシステムを強制的にパワーオフする（ステップS311）。また、データロック状態が解除できないHDD15がドッキングステーションに設けられたものである場合には、ブートストラップ処理が実行される（ステップS312）。

【0047】このように、ブートデバイス以外の他のハードディスクドライブがドッキングステーションに存在するものであるか、コンピュータ本体に存在するものであるかによってブート制御を切り替え、ドッキングステーションに存在するものであればそのデータロック状態を解除できない場合であってもブートストラップ処理を実行することにより、例えばネットワーク接続されたドッキングステーションにユーザ自身のコンピュータ本体を装着してデータ通信などを行う場合は、ドッキングステーション内に設けられた他人のハードディスクドライブの機密性を維持したまま、そのドッキングステーションの通信機能を利用するといった運用が可能となる。

【0048】

【発明の効果】以上説明したように、この発明によれば、データロック機能を有する複数のハードディスクドライブを使用可能な環境下においてそれらハードディスクドライブそれぞれの用途の違いやその接続環境の違いなどを考慮したパスワードチェック処理を実行できるようになり、システム全体の総合的なセキュリティレベルを向上することが可能となる。

【図面の簡単な説明】

【図1】 この発明の一実施形態に係るコンピュータシステムの構成を示すブロック図。

【図2】 同実施形態のコンピュータシステムの他の構成例を示すブロック図。

【図3】 同実施形態で使用されるHDDパスワード制御処理の第1の手順を示すフローチャート。

【図4】 同実施形態で使用されるHDDパスワード制御

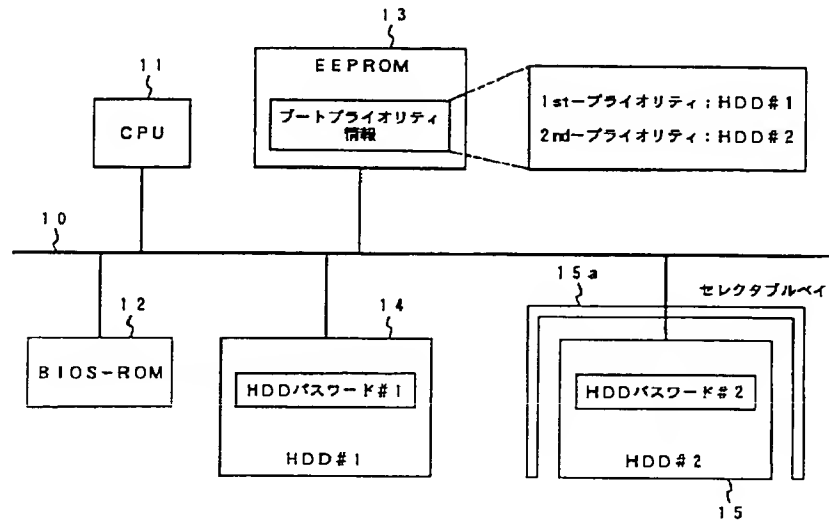
処理の第2の手順を示すフローチャート。

【図5】 同実施形態で使用されるHDDパスワード制御処理の第3の手順を示すフローチャート。

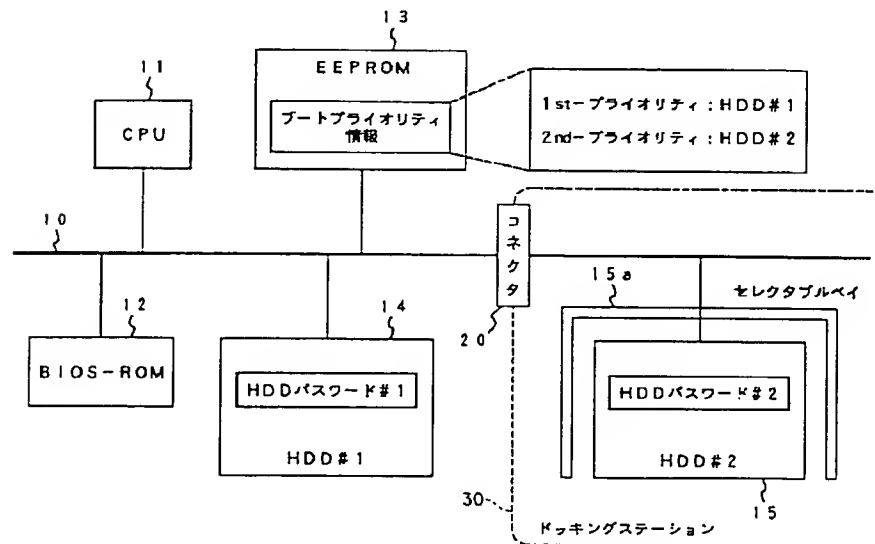
【符号の説明】

11…CPU、12…BIOS-ROM、13…EEPROM、14…1st-プライオリティのHDD、15…2nd-プライオリティのHDD、15a…セレクトابلベイ、30…ドッキングステーション。

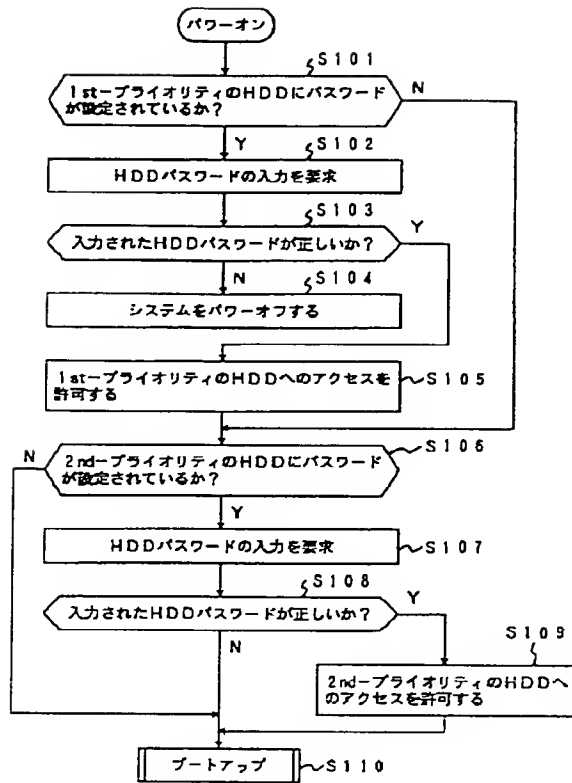
【図1】



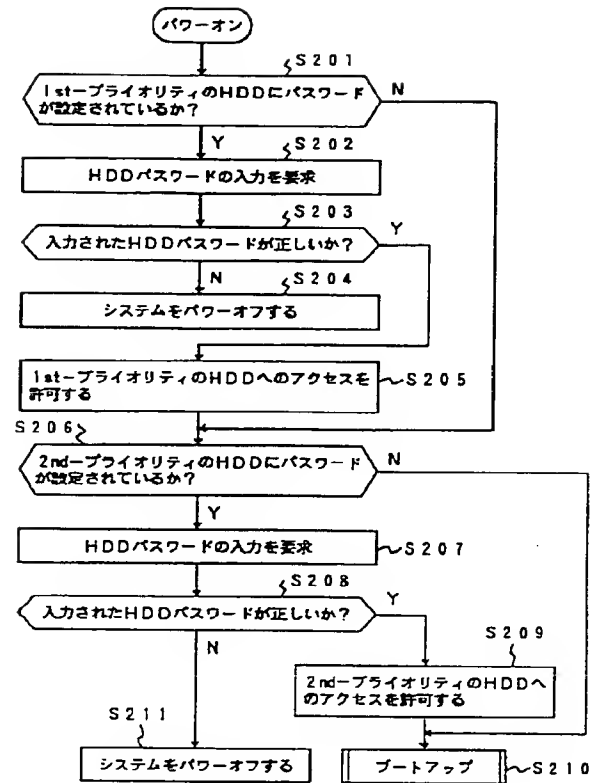
【図2】



【図3】



【図4】



【図5】

